

Муниципальное
дошкольное
учреждение детский сад № 33 села
Вознесенское
муниципального
Хабаровского края

бюджетное
образовательное
Амурского
района

УТВЕРЖДЕНА
Приказом заведующего
МБДОУ № 33 с. Вознесенское

от « 07 » апреля 20 22 г. № 46-1/

Е.А. Жихарева



**Модель угроз
безопасности персональных данных
при их обработке в информационных системах**

Содержание

Определения	3
Обозначение и сокращения	6
Введение	7
Классификация нарушителей	9
Предположения об имеющихся у нарушителя средствах реализации угроз	11
Вероятность реализации угрозы безопасности персональных данных	12
Виды угроз	12
Модель угроз безопасности	18
Заключение	22

Введение

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПД н строится на основании [отчета о результатах проведения внутренней проверки](#).

В модели угроз представлено описание структуры ИСПД н, состава и режима обработки ПД н, классификацию потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПД н включает: Описание угроз. Оценку вероятности возникновения угроз. Оценку реализуемости угроз. Оценку опасности угроз. Определение актуальности угроз

. В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз.

Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса

средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для

осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, кон-струкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПД н) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные,

доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД и (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и средства защиты информации, применяемые в информационных системах

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующей отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

Программное (программно-математическое) воздействие –

несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПД н – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПД н – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПД н – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПД н – угрозы безопасности персональных данных

1. ИСПД н и Структура ИСПД н

Таблица 1 – Параметры ИСПД н

Заданные характеристики безопасности персональных данных	Типовая информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности.

Состав и структура персональных данных

В ИСПД н обрабатываются [следующие персональные данные](#):

- Фамилия, имя, отчество.
- Место, год и дата рождения.
- Адрес места жительства.
- Паспортные данные.
- Образование.
- Информация о трудовой деятельности, о трудовом стаже.
- Домашний, мобильный телефон.
- Сведения о составе семьи.
- Сведения о воинском учёте.
- Результат обязательного медицинского осмотра.
- Копии приказов по личному составу.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к 3 **категории персональных данных**, т.е. к данным, позволяющим идентифицировать субъекта персональных данных.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, удаление, уничтожение персональных данных.

Все пользователи ИСПД н имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа

в таблице 2.

Таблица 2 – Матрица доступа

Группа	Уровень доступа к ПД н	Разрешенные действия	Сотрудники отдела
Администратор безопасности	<p>Обладает правами Администратора ИСПД н</p> <p>Обладает полной информацией об ИСПД н</p> <p>Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПД н</p> <p>Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных)</p>	<ul style="list-style-type: none"> - сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение 	Программист
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	<ul style="list-style-type: none"> - сбор - систематизация - накопление - хранение - уточнение - использование - 	Работники отдела приема и выдачи документов, работники отдела приватизации, юрист

Классификация нарушителей

По признаку принадлежности к ИСПД н все нарушители делятся на две группы:

Внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД н;

Внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД н.

4.1. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны МБДОУ № 33 с.Вознесенское.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПД н, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

4.2. Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПД н обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПД н в соответствии с принятой политикой информационной безопасности (правилами).

К внутренним нарушителям могут относиться:

- администратор безопасности ИСПД н (категория I);
- пользователи ИСПД н (категория II);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПД н, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал ЛПУ (водитель, уборщик помещений) (категория VII);
- уполномоченный персонал разработчиков ИСПД н, который на договорной основе, имеет право на техническое обслуживание и модификацию компонентов ИСПД н (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПД н для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПД н. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПД н, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПД н в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ.

Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПД н должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий V-VIII относятся к вероятным нарушителям. Предполагается, что возможность

сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

общая информация – информации о назначения и общих характеристиках ИСПД н; *эксплуатационная информация* – информация, полученная из эксплуатационной документации;

чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПД н (например, сведения из проектной документации ИСПД н).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПД н;

- сведения об информационных ресурсах ИСПД н: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПД н;

- данные о реализованных в ПСЗИ принципах и алгоритмах; - исходные тексты программного обеспечения ИСПД н;

- сведения о возможных каналах реализации угроз; - информацию о способах реализации угроз.

Предполагается, что лица категории V и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПД н и функционально

ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПД н. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПД н в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет: аппаратные компоненты СЗПД н и СФ СЗПД н;

доступные в свободной продаже технические средства и программное обеспечение; специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ЛПУ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПД н предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

средств перехвата технических каналов утечки;

средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
 средств воздействия на источники и через цепи питания; средств воздействия через цепи заземления;
 средств активного воздействия на технические средства (средств облучения). Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

Исходный уровень защищенности ИСПД н

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПД н (Y_1).

В таблице представлены характеристики уровня исходной защищенности для ИСПД н

Таблица 1 – Исходный уровень защищенности

Позиция	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	
2	По наличию соединения с сетями общего пользования	
3	По встроенным (легальным) операциям с записями баз персональных данных	
4	По разграничению доступа к персональным данным	
5	По наличию соединений с другими базами ПД н иных ИСПД н	
6	По уровню (обезличивания) ПД н	
7	По объему ПД н, которые предоставляются сторонним пользователям ИСПД н без предварительной обработки	

Вероятность реализации УБПД н

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПД н для ИСПД н в складывающихся условиях обстановки.

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПД н недостаточны ($Y_2 = 5$);

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПД н не приняты ($Y_2 = 10$).

При обработке персональных данных в ИСПД н можно выделить следующие угрозы:

1. Угрозы утечки информации по техническим каналам 2. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПД н, при обработке ПД н в ИСПД н, возможно при наличии функций голосового ввода ПД н в ИСПД н или функций воспроизведения ПД н акустическими средствами ИСПД н.

В ИСПД н учреждения МБДОУ № 33 с. Вознесенское функции голосового ввода ПД н или функции воспроизведения ПД н акустическими средствами отсутствуют.

Вероятность реализации угрозы – **маловероятна**.

3. Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники,

информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПД н.

В учреждении введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи.

Вероятность реализации угрозы – **маловероятна**.

4. Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение); - нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

5. Угрозы уничтожения, хищения аппаратных средств ИСПД н носителей информации путем физического доступа к элементам ИСПД н, кража ПЭВМ.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД н.

В учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятной**.

6. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, ведется учет и хранение носителей в запираемом шкафу.

Вероятность реализации угрозы – **маловероятна**.

7. Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, организовано хранение ключей в запираемом шкафу и введена политика «чистого стола».

Вероятность реализации угрозы – **маловероятна**.

8. Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД н и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

9. Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

10. Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПД н.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, пользователи ИСПД н проинструктированы о работе с ПД н.

Вероятность реализации угрозы – **маловероятна**.

11. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). Действия вредоносных программ (вирусов).

Программно-математическое воздействие - это воздействие с помощью вредоносных программ.

Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее

выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

- исказить произвольным образом, заблокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В Учреждении на всех элементах ИСПД н установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – **низкая**.

12. Недекларированные возможности системного ПО и ПО для обработки персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В Учреждении нет программного обеспечения разрабатываемого собственными разработчиками/сторонними специалистами.

Вероятность реализации угрозы – **маловероятна**.

13. Установка ПО не связанного с исполнением служебных обязанностей.

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПД н или ее элементов.

В Учреждении введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО. Вероятность реализации угрозы – **маловероятна**.

14. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПД н и СЗПД н в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

15. Утрата ключей и атрибутов доступа.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают

ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – **низкая**.

16. Непреднамеренная модификация (уничтожение) информации сотрудниками. Угроза осуществляется за счет действия человеческого фактора пользователей ИС-

ПД н, которые нарушают положения принятых правил работы с ИСПД н или не осведомлены о них.

В Учреждении осуществляется резервное копирование обрабатываемых ПД н, пользователи проинструктированы о работе с ИСПД н.

Вероятность реализации угрозы – **маловероятна**.

17. Непреднамеренное отключение средств защиты.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД н, которые нарушают положения принятых правил работы с ИСПД н и средствами защиты или не осведомлены о них.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПД н.

Вероятность реализации угрозы – **маловероятна**.

18. Выход из строя аппаратно-программных средств.

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении осуществляет резервирование ключевых элементов ИСПД н.

Вероятность реализации угрозы – **маловероятна**.

19. Сбой системы электроснабжения.

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении ко всем ключевым элементам ИСПД н подключены источники бесперебойного питания и осуществляет резервное копирование информации.

Вероятность реализации угрозы – **маловероятна**.

20. Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна**.

21. Угрозы преднамеренных действий внутренних нарушителей.

Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке.

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПД и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

22. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД и, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В Учреждении пользователи осведомлены о порядке работы с персональными данными, а так же подписали Договор о неразглашении.

Вероятность реализации угрозы – **маловероятна**.

23. Угрозы несанкционированного доступа по каналам связи.

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПД и, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИС-ПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

Перехват в пределах контролируемой зоны внешними нарушителями

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок..

Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внутренними нарушителями.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

24. Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Вероятность реализации угрозы – **маловероятна**.

25. Угрозы внедрения по сети вредоносных программ.

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть: программы подбора и вскрытия паролей;

программы, реализующие угрозы;

программы, демонстрирующие использование недеklarированных возможностей программного и программно-аппаратного обеспечения ИСПД н;

программы-генераторы компьютерных вирусов;

программы, демонстрирующие уязвимости средств защиты информации и др. Вероятность реализации угрозы – **маловероятна**. Модель угроз безопасности МБДОУ № 33с. Вознесенское

Исходный класс защищенности – 3.

Таблица 2 – Угрозы безопасности

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
---------------------	------------------------------------	-----------------------------------	------------------	---------------------

1. Угрозы от утечки по техническим каналам				
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная
2. Угрозы несанкционированного доступа к информации				
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПД и носителей информации путем физического доступа к элементам ИСПД и				
2.1.1. Кража ПЭВМ	Маловероятно	Низкая	Низкая	Неактуальная
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная
2.1.4. Кражи, модификации, уничтожения информации	Маловероятно	Низкая	Низкая	Неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе				
2.2.1. Действия вредоносных программ (вирусов)	Маловероятно	Низкая	Низкая	Неактуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПД н в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.				
2.3.1. Утрата ключей и атрибутов	Маловероятно	Низкая	Низкая	Неактуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная

2.4. Угрозы преднамеренных действий внутренних нарушителей				
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее	Маловероятно	Низкая	Низкая	Неактуальная
2.5. Угрозы несанкционированного доступа по каналам связи				
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПД и принимаемой из внешних сетей				
2.5.1.1. Перехват за пределами контролируемой зоны;	Маловероятно	Низкая	Низкая	Неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная
2.5.1.3. Перехват в пределах контролируемой зоны внутренними	Маловероятно	Низкая	Низкая	Неактуальная
2.5.2. Угрозы сканирования, направленные на выявление типа или	Маловероятно	Низкая	Низкая	Неактуальная
2.5.3. Угрозы выявления паролей по сети.	Маловероятно	Низкая	Низкая	Неактуальная
2.5.4. Угрозы навязывание ложного маршрута сети	Маловероятно	Низкая	Низкая	Неактуальная
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная
2.5.6. Угрозы внедрения ложного объекта как в ИСПД и так и во внешних	Маловероятно	Низкая	Низкая	Неактуальная
2.5.7. Угрозы типа «Отказ в	Маловероятно	Низкая	Низкая	Неактуальная

2.5.8. Угрозы удаленного запуска приложений.	Маловероятно	Низкая	Низкая	Неактуальная
2.5.9. Угрозы внедрения по сети вредоносных программ.	Маловероятно	Низкая	Низкая	Неактуальная

Заключение

В соответствии с Порядком проведения классификации информационных систем персональных данных, на основании категории и объема обрабатываемых персональных данных – ИСПД н в МБДОУ № 33 с. Вознесенское классифицируется как ИСПД н класса КЗ.

Аттестация ИСПД н МБДОУ № 33 с. Вознесенское (не) требуется

